UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,366	10/14/2003	William Joseph Eakin	10018596-1	4386

22879 7590 11/07/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
DAGOSTA, STEPHEN M	
ART UNIT	**PAPER NUMBER**
2683	

DATE MAILED: 11/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/685,366	EAKIN, WILLIAM JOSEPH	
	Examiner	Art Unit	
	Stephen M. D'Agosta	2683	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 10-25-2005 have been fully considered but they are not persuasive.

1. The applicant argues that there is no motivation to combine. The primary examiner disagrees for several reasons. Firstly, the applicant appears to read to an extremely deep level in the cited prior art so as to render it un-combinable. The art cited both disclose, at a high level, a user attempting to remotely access a database thru wireless means in a secure manner. If the applicant were to re-read the paragraphs/columns cited by the examiner (and only those paragraphs), they would see that the cited art combines to arrive at the claim limitations. Secondly, the art is from similar fields of endeavor and solves similar problems which means a proper combination. Thirdly, secure remote access to a database is well known in the art and the prior art discloses this fact. Fourth, the claims recite a technology which reads on Remote Access Server, or RAS – this is an old technology which has been supported for years by companies such as Shiva, Microsoft, Cisco, Nortel, etc.. Lastly, the applicant's claims are written in a fashion that is broad enough to allow the examiner to broadly interpret them such that the prior art reads on the claims. Hence the applicant is invited to amend their claims such that they do not read on the prior art.

2. The applicant argues there is no reasonable expectation of success. Again, the applicant has chosen to not read the passages cited by the examiner which shows how one skilled would use the combination.

Also, the applicant appears to attack the references individually (applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986)). The office action clearly shows what Garrison teaches and fails to teach and then how Rezvani remedies the failing(s).

3. The applicant argues (claim 1) that the prior art does not teach an device ID. The examiner disagrees since the combined Garrison/Rezvani disclose use of the Internet which uses IP Addressing that uniquely identifies a user/device. Secondly, a logon/password also identifies a user.

4. The applicant argues claim 12 (RF transmission of ID). See #3 above and Garrison/Rezvani teaches use of wireless/RF transmission.

5. The applicant argues claims 189, 22, 24 and 25 do not disclose a multiple use ID. The examiner disagrees since he pointed out that both an IP Address and ESN can be used to both uniquely identify the user as well as if they are an authorized user (eg. security check of IP Address/ESN to see if it is an authorized user). Further, Garrison and Rezvani both teach connecting to the Internet which use devices such as Firewalls to authenticate users.

6. The new claims are broad enough to be combined with the prior independent/dependent claims (see attached office action).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-~~26~~ to 31 rejected under 35 U.S.C. 103(a) as being unpatentable over Garrison US 2002/0069355 and further in view of Rezvani et al. US 2002/0077077.

As per **claims 1, 12, 19, 22 and 24-25 and 27**, Garrison teaches a method for communicating information from a private database to a wireless communication device (abstract, figure 1 and Para#33 teaches wireless communications), comprising:

receiving a private database access request from the wireless communication device, (figure 4a-b and Para#42 teaches Username/Password which uniquely ID's the user/device) ;

comparing the password with a security indicia, the security indicia associated with the wireless communication device (figure 3 teaches a Password table #55 which is checked as does figures 4a-b), and

communicating the information from the private database to the wireless communication device when the appliance ID corresponds to the security indicia (figures 4a-b teaches authenticating the user and sending the data if the user is verified) **but is silent on** the private database access request including at least an appliance identification (ID) that uniquely identifies the wireless communication device and comparing the appliance ID with security indicia.

Garrison teaches authenticating a user via username and password, as pointed out by the primary examiner above. Garrison discloses use of many different communications networks (see Para#33) and one skilled understands that this would encompass use of the Internet. Hence the client's device/computer would use TCP/IP addressing which would inherently uniquely identify the appliance ID.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

With further regard to claims 19 and 22 and 30-31, Garrison teaches use of password authentication and RF transmissions while Rezvani teaches use of an ESN number which reads on applicant's use of term "multiple use" (see claim 2 below as well) and transmitter/processor (see figure 1).

With further regard to claim 24, Garrison teaches a computer system/program executed on client and server (figures 2-3) with software logic shown in figures 4a-b)

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the private database access request including at least an appliance identification (ID) that uniquely identifies the wireless communication device and comparing the appliance ID with security indicia, to provide added security checking of both login/password and device ID.

As per **claims 2 and 13,** Garrison teaches claim 1/12, **but is silent on** wherein the appliance ID is multiple-use identification indicia that is included in all communications from the wireless communication device.

Rezvani teaches authenticating a user via an ESN number of a cellular phone (Para #4 and 6) which reads on the applicant's use of the term "multiple-use identification" ("Appliance ID 210 is a serial number, phone number, security code, or other suitable unique identifier, of the cell phone 102 that uniquely identifies cell phone 102. Accordingly, the appliance ID 210 is referred to herein as a multiple-use unique identifier since the appliance ID 2 1 0 uniquely identifies the appliance and identifies the appliance as an authorized device to embodiments of the private database wireless access system").

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the appliance ID is multiple-use identification indicia that is included in all communications from the wireless communication device, to provide means for an ID to have multiple uses (ie. used as a phone number, security check, etc.)

As per **claims 3, 14 and 26,** Garrison teaches claim 2/13/25 **but is silent on** wherein the multiple-use identification indicia and the security indicia correspond to a telephone number of the wireless communication device.

Rezvani teaches authenticating a user via an ESN number of a cellular phone (Para #4 and 6) which reads on using the telephone number/MIN of the phone since both uniquely identify the user and can be used interchangeably.

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that wherein the multiple-use identification indicia and the security indicia correspond to a telephone number of the wireless communication device, to provide for associating a user to their phone for security purposes (eg. that one user will use that one phone).

As per **claim 4,** Garrison teaches claim 1 **but is silent on** wherein the appliance ID is a unique identifier included in a header information of the private database access request from the received wireless communication device.

Rezvani teaches transmitting data/header to a remote system that includes transmission of information including identification information (Para#66 and figure 4, #254/#258).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the appliance ID is a unique identifier included in a header information of the private database access request from the received wireless communication device, to provide means for transmitting the appliance ID in the overhead of a message header.

As per **claim 5,** Garrison teaches claim 1, wherein communicating further comprises transmitting the information radio frequency (RF) signal to the wireless communication device.

As per **claim 6,** Garrison teaches claim 1, wherein receiving the private database access request further comprises receiving information selecting one of a plurality of different private databases wherein the selected private database is communicated to the wireless communication device when the appliance ID corresponds to the security indicia (figures 4a-b teach the user being verified and then having access to databases, figure 1, 20a-d).

As per **claims 7 and 15-16,** Garrison teaches claim 1/13, further comprising;

receiving a second private database access request from a second wireless communication device (Para #3 teaches authorized access by users), the second private database access request including at least a password generated by a user (Para#42);

comparing the received password with a security code, the security code uniqtlely associated with the user (Para#42); and

but is silent on associating a second security indicia with a second unique appliance ID of the second wireless communication device when the received password corresponds to the security code, so that the private database is communicated to the second wireless communication device.

Garrison teaches authenticating a user via username and password, as pointed out by the primary examiner above. Garrison discloses use of many different communications networks (see Para#33) and one skilled understands that this would encompass use of the Internet. Hence the client's device/computer would use TCP/IP addressing which would inherently uniquely identify the appliance ID.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that associating a second security indicia with a second unique appliance ID of the second wireless communication device when the received password corresponds to the security code, so that the private database is communicated to the second wireless communication device, to provide means for the system to support access by a plurality of users based on their device ID and/or login/password.

As per **claim 8,** Garrison teaches claim 7, **but is silent on** further comprising saving the second unique appliance ID as the second security indicia uniquely associated with the second wireless communication device.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). The ESN is stored until the phone roams away and/or is shutoff. Hence the second appliance ID would be stored by the network/database until the user terminates contact.

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it saves the second unique appliance ID as the second security indicia uniquely associated with the second wireless communication device, to

provide means for keeping a user and user's device ID on record for security tracking/verification purposes.

As per **claim 9,** Garrison teaches claim 7, further comprising:

receiving a subsequent private database access request from the second wireless communication device (figures 4a-b) **but is silent on** the subsequent private database access request including at least the second unique appliance ID,

comparing the second unique appliance ID with the second security indicia, and

communicating the private database to the second wireless communication device when the second unique appliance ID corresponds to the second security indicia.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the subsequent private database access request including at least the second unique appliance ID, AND comparing the second unique appliance ID with the second security indicia, AND communicating the private database to the second wireless communication device when the second unique appliance ID corresponds to the second security indicia, to provide means for supporting a plurality of users who can be verified before accessing the database.

As per **claim 10,** Garrison teaches claim 1, further comprising:

uniquely associating a plurality of unique passwords with a plurality of unique passwords (figure 3, #55 and Para#42)

wherein one password uniquely identifies one of a plurality of wireless communication devices and wherein each of the security indicia are uniquely associated with one of a plurality of private databases (figure 1 shows multiple databases),

receiving the private database access request from one of the plurality of wireless communication devices, the private database access request comprising at least the password of the transmitting wireless communication device and an access request to a selected private database selected from the plurality of private databases (figures 4a-b),

comparing the password of the transmitting wireless communication device with the plurality of unique security indicia (figures 4a-b); and

communicating the selected private database to the transmitting wireless communication device when the password corresponds to the security indicia of the selected private database (figures 4a-b) **but is silent on**

use of appliance IDs which are check/verified to initiate access to database(s).

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it uses appliance IDs which are check/verified to initiate access to database(s), to provide means for multiple levels of security verification to include device ID, login, password, etc..

As per **claims 11 and 18,** Garrison teaches claim 1/12, further comprising receiving a communication from the wireless communication device that prevents association of the password with the security indicia so that communicating the private database to the wireless communication device is prevented (Para#42 and figures 4a-b) **but is silent on** use of an appliance ID.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it uses appliance IDs which are check/verified to initiate access to database(s), to provide means for multiple levels of security verification to include device ID, login, password, etc..

As per **claim 17 and 29,** Garrison teaches claim 12/27 **but is silent on** further comprising:

selecting a portion of the received private database using a browser, and

displaying the selected portion of the received private database on a display residing on the wireless communication device using the browser.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access and view a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134). Note Para#108 specifically teaches "..client device 22 may include, for example, an Internet browser application that may be used to access web pages via communications network 16".

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that selecting a portion of the received private database using a browser, AND displaying the selected portion of the received private database on a display residing on the wireless communication device using the browser, to provide support for Internet access.

As per **claim 20,** Garrison teaches claim 19, further comprising a memory configured to store the received private database (figure 2 is the client device which comprises a memory, #22).

As per **claim 21,** Garrison teaches claim 19, further comprising:

a display (figure 2, #29) **but is silent on** a browser configured to display the received private database on the display.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access and view a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134). Note Para#108 specifically teaches "..client device 22 may include, for example, an Internet browser application that may be used to access web pages via communications network 16".

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it uses a browser configured to display the received private database on the display, to provide means for access via the Internet.

As per **claim 23,** Garrison teaches claim 22 further comprising security code corresponding to a user associated with the private database, so that when the received ID is not initially associated with the security indicia, a password provided by the user of the remote wireless communication device causes the multiple-use unique ID to be associated with the security indicia when the password corresponds to the security code (Para#42 teaches use of login/password which is associated with the user's device).

As per **claim 28**, Garrison teaches claim 27 further comprising transmitting via both Internet and RF communications, the information from the remote database to the PWCD (figure 1 and Para #33 shows connections from the user to the remote database. Since Garrison teaches both wired/wireless technology, one skilled understands that the mobile user will send an RF message which will eventually be connected to a wired/Internet connection that connects to the database server).

Claim 32 rejected under 35 U.S.C. 103(a) as being unpatentable over Garrison/Rezvani and further in view of Schneider et al. US 6,178,505.

As per **claim 32**, Garrison teaches claim 27 comprising authenticating, without a user of the PWCD entering a password, whether the PWCD is authorized to access the information stored in a remote database.

Schneider teaches authentication, albeit poor, via just an IP Address:

As is clear from the above list of identification information, the degree to which a firewall can trust identification information to authenticate a user depends on the kind of identification information. For example, the IP address in a packet can be changed by anyone who can intercept the packet; consequently, the firewall can put little trust in it and authentication by means of the IP address is said to have a very low trust level. On the other hand, when the identification information comes from a token, the firewall can give the identification a much higher trust level, since the token would fail to identify the user only if it had come into someone else's possession. (C3, L16-27)

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that a password is not required, to provide means for different levels of security.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen M. D'Agosta whose telephone number is 571-272-7862. The examiner can normally be reached on M-F, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bill Trost can be reached on 571-272-7872. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Stephen D'Agosta
Primary Examiner